98P7839

(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) Veröffentlichungsnummer: **0 557 566 A1**

(12) EUROPÄISCHE PATENTANMELDUNG

(21) Anmeldenummer: 92103482.3

(22) Anmeldetag: 28.02.92

(51) Int. Cl.5: H04Q 11/04, H04Q 3/545, H04M 3/42

(43) Veröffentlichungstag der Anmeldung: **01.09.93 Patentblatt 93/35**

(84) Benannte Vertragsstaaten: **DE FR GB IT**

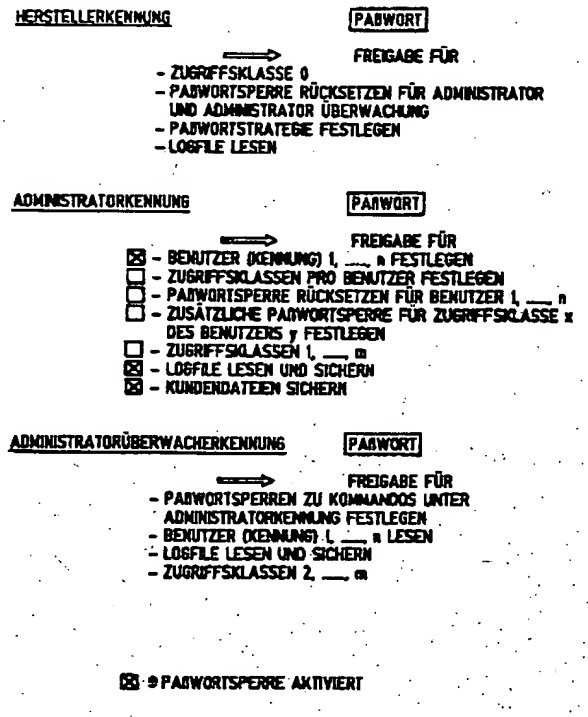
(71) Anmelder: **SIEMENS AKTIENGESELLSCHAFT**
Wittelsbacherplatz 2
D-80312 München(DE)

(72) Erfinder: **Wöss, Friedrich, Dipl.-Ing.**
Sternstrasse 11
W-8156 Otterfing(DE)
Erfinder: **Mages, Josef**
Ludwig-Berger-Strasse 26
W-8423 Abensberg(DE)

(54) Verfahren zur hierarchisch administrierbaren kennungsorientierten Freigabesteuerung für bedieneraufgabenbezogene Zugriffsanweisungen auf eine Datenbasis einer programmgesteuerten Kommunikationsanlage.

(57) Zum Schutz vor Zugriffen durch Unberechtigte ist für die Betriebstechnik-Schnittstelle einer programmgesteuerten Kommunikationsanlage eine hierarchisch strukturierte, kennungsorientierte Freigabesteuerung vorgesehen, die mit "Spezialkennungen" administrierbar ist. Als "Spezialkennungen" sind im einzelnen eine Administratorkennung vorgesehen, mit der im wesentlichen zugriffsberechtigte Benutzer, sowie deren individuelle Funktionsberechtigungen festgelegt werden können. Mit einer Administrator-Überwacherkennung lassen sich Erfordernisse festlegen, die erfüllt sein müssen, bevor die unter der Administratorkennung beabsichtigten Vorgänge ausgeführt werden. Eine Freigabe von Leistungsmerkmalen der programmgesteuerten Kommunikationsanlage ist nur mit einer Herstellerkennung möglich. Aufgrund der mit den einzelnen Spezialkennungen erzielbaren Flexibilität der Freigabesteuerung wird eine optimale Anpassung an die Sicherheitsbedürfnisse eines jeweiligen Anlagenbetreibers erreicht.

FIG 5



EP 0 557 566 A1

Programmgesteuerte Kommunikationsanlagen dienen in Kommunikationssystemen zur Verbindung von Endgeräten untereinander und zur Verbindung dieser Endgeräte mit Kommunikationsnetzen.

Die Vielfalt bekannter Kommunikationssysteme reicht von einfachen Telefonsystemen für die ausschließliche Übertragung von Sprache bis hin zu komplexen ISDN-Kommunikationssystemen (Integrated Services Digital Network) mit simultaner Mehrfach- oder auch Mischkommunikation von Sprache, Text, Bild und Daten.

An die Kommunikationsanlage im ISDN-Kommunikationssystem sind Endgeräte mit vielfältigen Leistungensmerkmalen anschließbar - von analogen und digitalen Telefonen, Fernkopierern, multifunktionalen Terminals, Arbeitsplatzsystemen, Personalcomputern, Teletext- und Bildschirmtextstationen, bis hin zu Datenterminals.

Aus einer Sonderausgabe von "Telcom report" - ISDN im Büro - 1985, ISBN 3-8009-3846-4, Siemens Aktiengesellschaft, ist ein derartiges Kommunikationssystem bekannt.

Die solchen Kommunikationssystemen zugrundeliegende Kommunikationsanlage ist modular aufgebaut und stellt im Prinzip eine digitale Datenverarbeitungsanlage mit einer Vielzahl von Peripherieeinheiten dar.

Zur Ausführung spezieller Dienste und Aufgaben sind im Rahmen eines sogenannten Server-Konzeptes modulare Einheiten - Server - vorgesehen, die mit eigener "Intelligenz" diese speziellen Aufgaben übernehmen.

So werden mit einem sogenannten Betriebs- und Datenserver zum Beispiel Leistungsmerkmale für ein elektronisches Datenbuch, für Funktionen zur Datenerfassung, Datenbearbeitung und Datentransport, sowie zur Durchführung von Steuerungsaufträgen angeschlossener Rechner, zur Verfügung gestellt.

Ein sogenannter Sprachinformationsserver bietet den angeschlossenen Teilnehmern die Möglichkeit, ihren Telefonanschluß auf persönliche Sprachpostfächer umzuleiten.

Ein Text- und Faxserver bietet unter anderem Leistungsmerkmale an, die eine Umsetzung von Teletext auf Telefax durchführen, wenn beim Empfänger kein telefaxfähiges Endgerät vorhanden ist.

Jeder dieser Server kann im Prinzip als eine für sich eigenständige Datenverarbeitungseinrichtung angesehen werden, die programmtechnisch und auch 'Hardware'-mäßig mit einer ebenfalls rechnergesteuerten Durchschalteeinheit der Kommunikationsanlage verbunden ist. An die Durchschalteeinheit, die gewissermaßen das Basismodul der Kommunikationsanlage bildet, sind die Endgeräte angeschlossen.

Der programmtechnische Teil der Kommunikationsanlage, allgemein mit System-Software bezeichnet, ist aufgaben- bzw. funktionsorientiert in eine Vermittlungstechnik-, eine Sicherheitstechnik- und eine Betriebstechnik-Software gegliedert. Zu jedem dieser Software-Module gehört in der Durchschalteeinheit sowie in den Servern jeweils eine Vielzahl von funktionsbezogenen Programm-Modulen, deren Abarbeitung in Form sogenannter 'Tasken' von einem Betriebssystem koordiniert werden.

Innerhalb der Vermittlungs-Software, die sich in die Funktionskomplexe Peripherietechnik, Leitungstechnik und Vermittlungstechnik unterteilen läßt, führt die Peripherietechnik im wesentlichen Daten- und Informations-Transportfunktionen aus.

Die Leitungstechnik hat die Aufgabe, die Schnittstelle zur Peripherietechnik an die ISDN-Schnittstelle zur Vermittlungstechnik anzupassen.

Die Vermittlungstechnik erbringt die eigentlichen Leistungen für die Benutzeroberfläche der Endgeräte bzw. für die Schnittstellen zu den verschiedenen Netzen.

Die Sicherheits-Software sammelt auftretende Fehlersignale aus Soft- und Hardware-Komplexen und veranlaßt die erforderlichen Schritte um Fehler zu beheben, fehlerhafte Funktionskomplexe durch andere zu ersetzen und entsprechende Fehlermeldungen auf einem Betriebsterminal zur Anzeige zu bringen.

Unter Betriebstechnik ist die Verwaltungs- und Wartungs-Software der Kommunikationsanlage zu verstehen, die dafür vorgesehen ist, um das Inbetriebssetzen und Inbetriebhalten sowie das Steuern des gesamten Kommunikationssystems zu ermöglichen. Dazu zählt auch das Laden von Programmen in die Kommunikationsanlage, das Verteilen und Starten dieser Programme in den verschiedenen Systemeinheiten, das Aktivieren und Deaktivieren von Systemfunktionen sowie das Erfassen und Archivieren aller betrieblichen Veränderungen des Gesamtsystems.

Die Betriebstechnik stellt gewissermaßen eine Schnittstelle zur Funktioneneinstellung einer programmgesteuerten Kommunikationsanlage dar. Um diese Schnittstelle im Sinne einer Bedienerfreundlichkeit unkompliziert und möglichst komfortabel auszugestalten, werden von der Kommunikationsanlage eine Vielzahl von Applikationsprogrammen zur Verfügung gestellt, die im wesentlichen dazu dienen, um nach Bedieneraufgaben formulierte Funktionsanweisungen in für die Betriebstechnik der Kommunikationsanlage verständliche betriebstechnische Einzelanweisungen umzusetzen. Die betriebstechnischen Einzelanweisungen sind nach vermittlungstechnischen Gesichtspunkten strukturiert und stellen gewissermaßen das Grundgerüst zur Einflußnahme auf die Kommunikationsanlage

dar.

Der Großteil der vorgesehenen betriebstechnischen Einzelanweisungen beeinflußt unmittelbar die in einer Datenbasis einer programmgesteuerten Anlage hinterlegten betriebstechnikbezogenen Informationen, die das Verhalten und die Funktionsweise der Kommunikationsanlage, z. B. gegenüber den einzelnen Kommunikationsteilnehmern, festlegen.

Aufgrund der nahezu unbegrenzten Einflußmöglichkeiten, die mit der Betriebstechnik-Schnittstelle zur Verfügung stehen und die insbesondere auch Zugriffe auf in eine ISDN-Kommunikationsanlage zwischenspeicherbare kommunikationsteilnehmerindividuelle Daten erlauben, darf die Betriebstechnik-Schnittstelle nur berechtigten Benutzern zugänglich sein.

Üblicherweise wird den berechtigten Benutzern jeweils ein Kennungscodewort mitgeteilt, das durch eine individuelles Paßwort ergänzt werden kann und in einen von den Benutzern nicht lesbaren Speicherbereich der datenverarbeitenden Einrichtung eingetragen wird. In den meisten Fällen werden diese Eintragungen von einem bereits berechtigten Benutzer oder vom Kundendienst-Personal der Herstellerfirma ausgeführt. Als Kennungscodeworte und Paßworte werden alphanumerische Zeichenfolgen verwendet.

In der Regel hat damit jeder Berechtigte die absolute Zugriffsberechtigung zum gesamten System. In vielen Fällen wirkt sich diese Tatsache nicht weiter störend aus, insbesondere dann nicht, wenn Eingriffe in die Betriebstechnik der Kommunikationsanlage äußerst selten anfallen, und keine schützenswerten Daten in der Kommunikationsanlage gespeichert werden. Dagegen genügt diese herkömmliche Art der undifferenzierten Vergabe von Zugangsberechtigungen nicht den Anforderungen solcher Anlagenbetreiber, die über die Betriebstechnik in ihrer Kommunikationsanlage häufig Änderungen vornehmen müssen, oder ihre Kommunikationsanlage auch als Datenverarbeitungseinrichtung im herkömmlichen Sinne benutzen.

Aufgabe der vorliegenden Erfindung ist es, für die Vergabe von Zugriffsberechtigungen ein Verfahren anzugeben, mit dem es einerseits möglich ist, eine äußerst komplexe Verteilung und Differenzierung der Zugriffsberechtigungen vorzugeben, das andererseits aber auch für solche Benutzer, deren Anforderungen bezüglich der Vergabe von Zugriffsberechtigungen gering sind, keinen Aufwand erfordert.

Gelöst wird diese Aufgabe erfindungsgemäß durch die Merkmale des Patentanspruchs 1.

Der wesentliche Vorteil des erfindungsgemäßen Verfahrens ist in seiner Flexibilität und in der Individualität zu sehen, wie den Sicherheitsbedürfnissen eines jeweiligen Anlagenbetreibers auf einfache Weise entsprochen werden kann. Da das erfindungsgemäße Verfahren unterschiedliche Aufgaben- und Funktionskomplexe mit individuellen Sicherheitsaspekten berücksichtigt, lassen sich auch mehrere im Prinzip voneinander unabhängige Funktionseinheiten gemeinsam durch ein Verfahren sicherheitstechnisch verwalten.

Vorteilhafte Weiterbildungen der Erfindung sind in den Unteransprüchen angegeben.

Zum detaillierten Verständnis der Erfindung und ihrer Weiterbildungen, insbesondere zur Darlegung weiterer vorteilhafter Aspekte wird im folgenden ein Ausführungsbeispiel der Erfindung anhand der Zeichnung näher beschrieben.

Dabei zeigen:

- FIG 1 in schematischer Blockdarstellung eines bekannten ISDN-Kommunikationssystems im Zusammenhang mit Peripheriegeräten,
- FIG 2 ein Schalenmodell zur Darstellung der Software-Architektur der bekannten Kommunikationsanlage,
- FIG 3 ein auf einem Betriebsterminal zur Anzeige kommendes Hauptverzeichnis von bedieneraufgabenbezogenen Zugriffsanweisungen,
- FIG 4 ein Beispiel für eine Zuordnung von Zugriffsanweisungen zu Zugriffsklassen,
- FIG 5 eine Auflistung von zur Administration vorgesehenen Funktionsfreigaben, und
- FIG 6 ein Beispiel für die in einer Benutzerkennungstabelle und Benutzerprofiltabelle vermerkten Einträge.

In FIG 1 ist eine bekannte Kommunikationsanlage zusammen mit einer Vielzahl von anschließbaren Geräten schematisch dargestellt. Wesentliche Bestandteile der Kommunikationsanlage sind eine Durchschalteeinheit SWU und eine Betriebs-Datenservereinheit ADS. Diese beiden Einheiten sind ergänzt durch eine Sprachinformations-Servereinheit VMS und eine Text-, Faxservereinheit TFS.

Prinzipiell sind diese Einheiten SWU, ADS, VMS, TFS als reine Software-Module aufzufassen, d. h. , daß die gewählte Darstellung nicht an eine bestimmte Art und Verteilung der verwendeten Hardware gebunden ist. Insbesondere kann der Durchschalteeinheit SWU und der Betriebs-Datenservereinheit ADS dieselbe Prozessoreinrichtung zugeordnet sein.

In einer Minimalkonfiguration setzt sich die Kommunikationsanlage funktional nur aus der Durchschalteeinheit SWU für die Durchschaltevermittlungsfunktionen und der Betriebs-Datenservereinheit ADS für die Speichervermittlungsfunktionen zusammen. Sämtliche Einheiten sind im Sinne eines Zusammenwirkens über einen Systembus miteinander verbunden.

Gegenüber der Durchschalteeinheit SWU, die im wesentlichen lediglich Informationswege verknüpft, stellt die Betriebs-Datenservereinheit ADS eine zusätzlich mit der Organisation, Steuerung, Verwaltung und Wartung der gesamten Kommunikationsanlage betraute Systemeinheit dar.

Die dazu in der Betriebs-Datenservereinheit ADS implementierten Funktionen lassen sich in einem systembetriebstechnischen Funktionskomplex und in verschiedene optionale Datenanwendungsfunktionen unterteilen. Zu den systembetriebstechnischen Funktionen zählen z. B. das Inbetriebsetzen der Anlage, das Laden von Systemprogrammen, das Verteilen und Starten dieser Systemprogramme, das Aktivieren bzw. Deaktivieren von Systemfunktionen, sowie das Erfassen aller betrieblichen Veränderungen. In den Bereich der Datenanwendungsfunktionen fallen im wesentlichen Datentransportfunktionen für einen Transport verschiedenartiger Daten, wie Gebührendaten und Systemanwenderdateien zwischen der Kommunikationsanlage und anderen Datenbearbeitungssystemen, ebenso wie Datenerfassungsfunktionen, z.B. für eine Gebührenermittlung, oder für verkehrsstatistische Daten und Datenbearbeitungsfunktionen, z.B. für eine Aufbereitung von ermittelten Daten.

Für die Ausführung von Funktionen wird eine Vielzahl von Programmen bereitgehalten, die bei Bedarf abgearbeitet werden. Zur Verwaltung dieser Programme dient sowohl ein Echtzeit-Betriebssystem, das im wesentlichen die systemtechnikbezogenen Programme verwaltet, als auch ein Teilnehmer-Betriebssystem (Timesharing-Betriebssystem), dem die auf die Datenanwendungsfunktionen bezogenen Programme zugeordnet sind.

Der simultane Betrieb eines Echtzeit-Betriebssystems und eines Teilnehmer-Betriebssystems in einer Kommunikationsanlage ist aus der europäischen Patentanmeldung: Aktenzeichen 89 104 481.0 bekannt.

Die Betriebs-Datenservereinheit ADS ist mit Speichereinrichtungen verbunden, in denen System- und Anwenderprogramme sowie verschiedenartige Daten, z.B. Gebührendaten und verkehrsstatistische Daten, gespeichert sind bzw. während des Betriebs der Anlage hinterlegt werden können. An die Betriebs-Datenservereinheit ADS sind des weiteren Bedienplätze, sogenannte Betriebsterminals BT, angeschlossen. Prinzipiell sind über ein Betriebsterminal BT Änderungen sämtlicher Konfigurationsdaten der gesamten Kommunikationsanlage möglich. Im wesentlichen werden jedoch über das Betriebsterminal BT Verwaltungs- und Wartungsaufgaben durchgeführt.

In FIG 2 ist anhand eines Schalenmodelles die Softwarearchitektur der Durchschalteeinheit SWU wie auch der Betriebs-Datenservereinheit ADS veranschaulicht. Unter der Verwaltung eines Betriebssystems OS nimmt die Durchschalteeinheit SWU die Funktionen der Vermittungssoftware, bestehend aus der Peripherietechnik PP, der Leitungstechnik DH und der Vermittlungstechnik CP war und beinhaltet zudem die die Sicherheitstechnik DEP und Betriebstechnik AM betreffenden Softwarekomplexe. Sämtliche Softwarekomplexe haben Zugriff auf eine Datenbasis DB, in der sämtliche veränderbare Konfigurationsdaten, d.h. Konfigurationsparameter, hinterlegt sind bzw. von der Software ausgelesen und eingetragen werden.

Die Betriebs-Datenservereinheit ADS steht mit der Software der Durchschalteeinheit SWU in enger Verbindung und weist ebenfalls von einem Betriebssystem OS verwaltete, der Vermittlungssoftware, der Sicherheitstechnik und der Betriebstechnik zugeordnete Softwarekomplexe (nicht dargestellt) auf. Zudem ist sie mit weiteren anwenderorientierten Softwarekomplexen versehen. So beinhaltet die Software der Betriebs- und Datenservereinheit ADS einen Komplex für Gebührenerfassung und -bearbeitung GCU, einen Softwarekomplex zur Realisierung eines elektronischen Telefonbuches ETB sowie einen Komplex zur Bildung einer Art Software-Schnittstelle MMI/EMML zur Umsetzung von bedieneraufgabenbezogenen Zugriffsanweisungen auf, von der Betriebstechnik AM ausführbare Einzelanweisungen. Diese Software-Schnittstelle wird häufig Mensch-Maschinen-Interface MMI genannt.

Außerdem umfaßt die Betriebs-Datenservereinheit ADS die Steuerung der systemtechnischen Peripherie, z.B. der angeschlossenen Speichereinrichtungen und der Betriebsterminals BT, sowie die Steuerung und den Anschluß der Kommunikationsanlage an eine DVA-Anlage. Zur Hinterlegung der variablen Daten, d.h. der Konfigurationsparameter, für die Softwarekomplexe der Betriebs-Datenservereinheit ADS ist wiederum eine Datenbasis DB vorgesehen.

Es sei an dieser Stelle noch bemerkt, daß die in der FIGUR vorgenommene Trennung zwischen Softwarekomplexen innerhalb der Durchschalteeinheit SWU und der Betriebs-Datenservereinheit ADS im wesentlichen nur den modularen Aufbau der Software verdeutlichen soll. In der Praxis stehen die Softwarekomplexe der Durchschalteeinheit SWU und der Betriebs-Datenservereinheit ADS zueinander in enger Verbindung, insbesondere ist die Software-Schnittstelle MMI/EMML auch eine Schnittstelle zur Betriebstechnik AM der Durchschalteeinheit SWU, in deren Datenbasis DB somit auch über die Software-Schnittstelle MMI/EMML Veränderungen vorgenommen werden können.

Im weiteren wird davon ausgegangen, daß der Zugriff auf die in der Betriebs-Datenservereinheit ADS befindlichen Softwarekomplexe der Gebührenerfassung und -verarbeitung GCU, des elektroni-

schen Datenbuchs ETB und der Software-Schnittstelle MMI/EMML einer kennungsorientierten Freigabesteuerung FS gemäß der Erfindung unterworfen sind.

Je nach Aufbaustufe der Kommunikationsanlage können zudem noch weitere Softwarekomplexe, z. B. für eine automatische Anrufverteilung (automatically call-distribution) und einer netzgesteuerten Konfiguration (network management-center), zum Konfigurieren einer Kommunikationsanlage über ein Kommunikationsnetz der kennungsorientierten Freigabesteuerung FS unterstellt werden.

In FIG 3 ist eine Bildschirmmaske dargestellt, die auf einem Bedienterminal BT zu Beginn einer Verwaltungs- oder Wartungssitzung erscheint. Einer Bedienperson wird, gesteuert durch die in der Betriebs-Datenservereinheit ADS befindliche Software-Schnittstelle MMI/EMML, ein nach Bedieneraufgaben gegliedertes Vorgehen ermöglicht. Die Softwareschnittstelle MMI/EMML sieht eine textunterstützte Bedienerführung vor und setzt eine von dem Bediener ausgewählte Bedieneraufgabe in eine Vielzahl von Einzelanweisungen, sogenannte AMO's (Administration Maintenance Order) um. Die wesentliche Aufgabe der Software-Schnittstelle MMI/EMML besteht damit darin, die Aufgaben, die ein Bediener an der Kommunikationsanlage ausführen möchte, als solche zu erfragen und in eine Sequenz von Einzelanweisungen (AMO's) zu übersetzen, die nach Programm- und Hardware-Strukturen orientiert sind, und in ihren einzelnen Funktionen, Wirkungen und Zusammenhängen nur von speziell geschultem Personal verstanden werden können. Jede der in der FIGUR aufgelisteten Objektgruppen läßt sich auswählen und in eine Vielzahl von bedieneraufgabenbezogenen Objektuntergruppen aufgliedern.

Zur funktionalen Klassifizierung können sämtliche von der Software-Schnittstelle MMI/EMML zur Verfügung gestellten bedieneraufgabenbezogenen Zugriffsanweisungen, sogenannten Zugriffsklassen, zugeordnet werden. In der Software-Schnittstelle MMI/EMML sind dazu spezielle Zuordnungsanweisungen vorgesehen, die ausschließlich einer eigenen Zugriffsklasse, die gewissermaßen eine privilegierte Zugriffsklasse darstellt, zugeordnet sind. Außerdem sind Zugriffsanweisungen, die ein Sperren und Freigeben von Leistungsmerkmalen der Kommunikationsanlage ermöglichen, ebenfalls ausschließlich einer eigenen Zugriffsklasse, die auch als privilegierte Zugriffsklasse bezeichnet werden kann, zugeordnet.

In FIG 4 soll die Zuordnung von Zugriffsanweisungen zu Zugriffsklassen anhand eines einfachen Beispiels aufgezeigt werden. Einer Zugriffsklasse 0, die im folgenden auch als erste privilegierte Zugriffsklasse bezeichnet wird, sind die Zugriffsanweisungen zugeordnet, die ein Sperren und Freigeben von Leistungsmerkmalen A,B,C ermöglichen. Einer Zugriffsklasse 1, die im weiteren auch als zweite privilegierte Zugriffsklasse bezeichnet wird, sind die Zuordnungsanweisungen zugeordnet, mit denen eine Zuordnung von Zugriffanweisungen zu Zugriffsklassen vorgenommen werden kann.

Einer weiteren Zugriffsklasse 2 sind z.B. Zugriffsanweisungen zugeordnet, die das Ändern und Tauschen von Teilnehmerrufnummern betreffen. Einer Zugriffsklasse 3 sind z.B. Zugriffsanweisungen zugeordnet, die das Abfragen der Anzahl amtsberechtigter Nebenstellen sowie das Abfragen und Ändern von Teilnehmerberechtigungen betreffen. Einer Zugriffsklasse 4 sind Zugriffsanweisungen zugeordnet, die unter anderem das Abfragen, Löschen und Einrichten von Teilnehmerdaten betreffen.

Zur selektiven Freigabesteuerung für bedieneraufgabenbezogene Zugriffsanweisungen sieht die Erfindung ein flexibles Verfahren vor, das an das Sicherheitsbedürfnis eines Anlagenbetreibers angepaßt werden kann, wodurch sich ein Sicherheitsspektrum abdecken läßt, das von einem bis zu einer beliebigen Anzahl von Berechtigten mit unterschiedlichen Zugriffsberechtigungen reicht. Jede Bedienperson, die an einem Bedienterminal BT der Kommunkationsanlage Verwaltungs- oder Wartungsaufgaben ausführen möchte, muß sich prinzipiell mit einer sogenannten Kennung gegenüber der Kommunikationsanlage identifizieren. In Abhängigkeit dieser Kennung sind die Bedienerpersonen jeweils zu unterschiedlichen Anlagenzugriffen berechtigt. Prinzipiell kann zu jeder Kennung ein Paßwort vorgesehen werden, das die Authentizität des die betreffende Kennung benutzenden Bedieners bestätigen soll.

In FIG 5 sind die zur Administration der Freigabesteuerung dienenden 'Spezialkennungen' zusammen mit den durch sie jeweils freigegebenen Funktionen bzw. Zugriffen aufgeführt.

Eine der drei Spezialkennungen, die im folgenden als Administratorkennung bezeichnet wird, ist immer, also unabhängig vom Schutzbedürfnis des Anlagenbetreibers vorgesehen. Mit der Administratorkennung, die durch ein Paßwort vor Mißbrauch geschützt werden kann, wird eine Freigabe für die zur Administratorkennung gehörig aufgelisteten Funktionen erteilt. Sollen mehrere Benutzer dazu berechtigt werden, verwaltungs- und wartungstechnische Aufgaben auszuführen, so wird für die berechtigten Benutzer jeweils eine Benutzerkennung festgelegt, die in einer Benutzerkennungstabelle vermerkt wird. Mit der Administratorkennung ist die Benutzerkennungstabelle natürlich auch für Änderungen freigegeben.

Des weiteren berechtigt die Administratorkennung zu jeder in der Benutzerkennungstabelle fest-

gelegten Benutzerkennung Zugriffsklassen zuzuordnen, die in einer Benutzerprofiltabelle als zu einer jeweiligen Benutzerkennung zugehörig vermerkt werden.

Mit der Administratorkennung können außerdem auch Paßwort-Sperren, die ein Benutzer zu seiner Benutzerkennung vorgesehen hat, rückgesetzt werden, wodurch die betreffende Paßwort-Sperre deaktiviert wird.

Unter der Administratorkennung kann auch zu jeder der einer jeweiligen Benutzerkennung zugeordneten Zugriffsklassen eine Freigabebedingung, z.B. eine Paßwort-Sperre, festgelegt werden. Mit einer Paßwort-Sperre erfolgt die Freigabe der betreffenden Zugriffsklasse nur dann, wenn ein anderer Benutzer - der mit dem Benutzer nicht identisch ist, unter dessen Benutzerkennung die Zugriffsklasse freigegeben werden soll - mit seinem Paßwort einer Freigabe zustimmt.

Weiterhin wird mit der Administratorkennung eine Freigabe für alle Zugriffsklassen, außer der Zugriffsklasse 0 (auch erste privilegierte Zugriffsklasse genannt), erteilt, d.h. daß alle den freigegebenen Zugriffsklassen zugeordneten Zugriffsanweisungen zur Verfügung stehen.

Die Administratorkennung berechtigt außerdem zum Lesen und Sichern einer Protokolldatei (Logfile), die vom Steuerungssystem der Kommunikationsanlage zyklisch erstellt wird, und in der wenigstens die während eines jeweiligen Zeitraumes mit den Spezialkennungen vorgenommenen Funktionen bzw. die Freigabesteuerung betreffenden Änderungen vermerkt werden.

Sind in der Kommunikationsanlage Kundendateien eingerichtet, dann berechtigt die Administratorkennung auch zur Abspeicherung dieser Kundendateien auf die an die Betriebs-Datenservereinheit ADS angeschlossenen Speichereinrichtungen.

Bei entsprechendem Sicherheitsbedürfnis kann eine weitere 'Spezialkennung', eine sogenannte AdministratorÜberwacherkennung eingerichtet werden, die im wesentlichen zur Kontrolle der unter der Administratorkennung vorgenommenen Vorgänge dient. Die AdministratorÜberwacherkennung kann in der Praxis z.B. einem Arbeitnehmervertreter zugeordnet werden, der damit eine gewisse Kontrollfunktion ausüben kann.

Mit der AdministratorÜberwacherkennung, die selbstverständlich auch durch ein Paßwort geschützt werden kann, können die unter der Administratorkennung ausführbaren Vorgänge gezielt mit Freigabebedingungen z.B. Paßwortsperren, belegt werden. Mit einer Paßwortsperre wird ein Vorgang unter der Administratorkennung nur dann freigegeben, wenn das der AdministratorÜberwacherkennung zugehörige Paßwort eingegeben wird, d.h. daß für den vom Administrator beabsichtigten Vorgang der AdministratorÜberwacher seine Zustimmung geben muß. In der dargestellten FIGUR ist ein solcher Paßwortschutz beispielhaft für das Festlegen der Benutzerkennungen sowie für das Lesen und Sichern der Protokolldatei als auch für das Sichern der Kundendateien vorgesehen.

Mit der AdministratorÜberwacherkennung wird des weiteren auch eine Freigabe dafür erteilt, die in der Benutzerkennungstabelle vermerkten Benutzerkennungen zu lesen. Des weiteren wird mit der AdministratorÜberwacherkennung eine Freigabe für alle Zugriffsklassen, außer der Zugriffsklasse 0 und der Zugriffsklasse 1 (vgl. Fig 4) erteilt. Auch ein Lesen und ein Sichern der Protokolldateien ist freigegeben.

Mit einer weiteren 'Spezialkennung', einer sogenannten Herstellerkennung, die dem Anlagenbetreiber in der Regel nicht zugänglich ist und im Regelfalle zur bei Inbetriebnahme und bei außergewöhnlichen Systemarbeiten und Umstellungen benutzt wird, wird eine Freigabe für die Zugriffsklasse 0 erteilt. Damit ist sichergestellt, daß nur der Hersteller selbst den Leistungsumfang der Kommunikationsanlage festlegen kann, und Leistungsmerkmale, die zwar softwaremäßig in der Anlage realisiert sind, vom Anlagenbetreiber jedoch nicht vertraglich erworben wurden, nicht ohne Kenntnis des Herstellers in Betrieb genommen werden können. Des weiteren ist mit der Herstellerkennung ein Rücksetzen der Paßwortsperren für die Administrator- und AdministratorÜberwacherkennung möglich, so daß z. B. bei Verlust des der Administratorkennung zugeordneten Paßwortes die Administratorkennung auch ohne Eingabe des zugeordneten Paßwortes zu den gewünschten Freigaben führt.

An dieser Stelle sei bemerkt, daß zu jeder Kennung, sofern mit ihr eine Freigabe bewirkt wurde, das bis zu diesem Zeitpunkt für diese Kennung geltende Paßwort geändert und die Paßwortsperre aktiviert oder deaktiviert werden kann. Letzteres bedeutet, daß die betreffende Kennung nicht paßwortgeschützt ist.

Mit der Herstellerkennung lassen sich des weiteren Paßwortstrategiemerkmale festlegen, insbesondere kann eingestellt werden, wieviele Zeichen (Buchstaben und Ziffern) eine Kennung aufweisen muß oder darf, oder wieviele Zeichen innerhalb eines Paßwortes gleich sein dürfen. Auch kann festgelegt werden, in welchen zeitlichen Abständen das Paßwort geändert werden muß, damit es seine Gültigkeit nicht verliert, und wieviele Fehlversuche bei einer Paßworteingabe zugelassen werden, bevor die betreffende Kennung gesperrt wird und wie lang diese Sperrzeit dann anhalten soll.

Mit der Herstellerkennung wird auch eine Freigabe für das Lesen der Protokolldatei erzielt. Ein Ändern oder Löschen der Protokolldatei ist mit der Herstellerkennung nicht vorgesehen; dadurch wird

bewußt verhindert, daß unter der Herstellerkennung vorgenommene Aktivitäten, die in der Protokolldatei aufgezeichnet werden, durch nachträgliches Abändern der Protokolldatei vertuscht werden können und damit nicht mehr nachweisbar bzw. nachvollziehbar wären.

In FIG 6 wird zur Veranschaulichung anhand eines Beispiels eine Zuordnung von Zugriffsklassen zu mehreren Benutzerkennungen dargestellt. Die Bildung von Benutzerkennungen wird natürlich nur dann vorgenommen, wenn die Sicherheitsbelange des Anlagenbetreibers es erfordern oder zulassen, mehrere Bedienerpersonen mit verwaltungs- und wartungsbezogenen Aufgaben zu betrauen. In der Darstellung der FIGUR sind insgesamt vier Benutzer vorgesehen, denen jeweils eine Benutzerkennung individuell zugeordnet ist. Diese Kennungen sind in einer Benutzerkennungstabelle BKT vermerkt. Wie bereits im Zusammenhang mit den 'Spezialkennungen' erwähnt, kann für jede Kennung eine Paßwortsperre aktiviert werden. Jede der Benutzerkennungen führt zur Freigabe von Zugriffsklassen, (d.h. zur Freigabe von den betreffenden Zugriffsklassen zugeordneten Zugriffsanweisungen), die zu jeder Benutzerkennung gehörig in einer Benutzerprofiltabelle BPT vermerkt sind. Zum Beispiel ist für die "Kundendienstkennung" eine Freigabe für die Zugriffsklasse 4, 5 und 6 vorgesehen. Eine Freigabe für die Zugriffsklassen 0 oder 1 ist mit Benutzerkennungen generell nicht möglich.

Jede der in der Benutzerprofiltabelle BPT zu einer jeweiligen Benutzerkennung vermerkten Zugriffsklassen ist mit einer Paßwortsperre versehbar, die unter der Administratorkennung festgelegt werden kann. Damit ist eine Freigabe der betreffenden Zugriffsklasse nur dann möglich, wenn das einer anderen Kennung zugeordnete Paßwort zusätzlich eingegeben wird. Im vorliegenden Beispiel ist eine Freigabe der Zugriffsklasse 5 unter der "Kundendienstkennung" nur möglich, wenn das vom Benutzer 4 gewählte Paßwort zusätzlich eingegeben wird. Eine Freigabe der Zugriffsklassen 4 und 6 erfolgt dagegen ohne zusätzliches Paßwort.

Patentansprüche

1. Verfahren zur hierarchisch administrierbaren kennungsorientierten Freigabesteuerung für bedieneraufgabenbezogene Zugriffsanweisungen auf in einer Datenbasis (DB) einer programmgesteuerten Kommunikationsanlage gespeicherte verwaltungs- und wartungsbezogene Systemkonfigurationsdaten, wobei die Zugriffsanweisungen an einem Betriebsterminal (BT) veranlaßt und jeweils in Form einer Abfolge von Einzelanweisungen von der Kommunikationsanlage ausgeführt werden, und die Zugriffsanweisungen im Sinne einer funktionalen Zugriffsklassifizierung jeweils einer oder mehreren Zugriffsklassen zuordenbar sind; als Kennungen sind:
   - eine Administratorkennung vorgesehen, mit der eine Zugriffsfreigabe auf die Zugriffsklassen und eine Freigabe zur Änderung
     – einer Benutzerkennungstabelle (BKT), in der zugriffsberechtigte Benutzerkennungen vermerkbar sind, und
     – einer Benutzerprofiltabelle (BPT) erfolgt, in der für diese Benutzerkennungen jeweils freigegebene Zugriffsklassen vermerkbar sind,
   - eine Administrator-Überwacherkennung vorsehbar, mit der eine Freigabe zur Einstellung von Freigabebedingungen erfolgt, unter denen die mit der Administratorkennung jeweils aus führbaren Änderungen freigegeben werden,
   - eine Herstellerkennung vorsehbar, mit der eine Zugriffsfreigabe für eine erste privilegierte Zugriffsklasse erfolgt, der den Leistungsumfang der programmgesteuerten Kommunikationsanlage einstellende Zugriffsanweisungen zugeordnet sind,
   - sowie Benutzerkennungen vorsehbar, mit denen eine Zugriffsfreigabe auf die in der Benutzerprofiltabelle für eine jeweilige Benutzerkennung als freigegeben vermerkten Zugriffsklassen erfolgt.

2. Verfahren nach Anspruch 1,
   dadurch gekennzeichnet,
   daß mit der Herstellerkennung eine Freigabe zum
   - Löschen von die Administrator- und AdministratorÜberwacherkennung betreffenden Paßwörtern und
   - zur Einstellung von Paßwortstrategiemerkmalen erfolgt.

3. Verfahren nach Anspruch 1 oder 2,
   dadurch gekennzeichnet,
   daß ausschließlich mit der Herstellerkennung eine Freigabe der ersten privilegierten Zugriffsklasse erfolgt.

4. Verfahren nach einem der vorhergehenden Ansprüche,
   dadurch gekennzeichnet,
   daß einer zweiten privilegierten Zugriffsklasse Änderungen der Zuordnung von Zugriffsanweisungen zu Zugriffsklassen bewirkende Zugriffsanweisungen zugeordnet sind.

5. Verfahren nach Anspruch 4,
dadurch gekennzeichnet,
daß ausschließlich mit der Administratorkennung eine Freigabe der zweiten privilegierten Zugriffsklasse erfolgt.

6. Verfahren nach einem der vorhergehenden Ansprüche,
dadurch gekennzeichnet,
daß mit der Administratorkennung eine Freigabe zur Einstellung von Freigabebedingungen erfolgt, unter denen mit einer jeweiligen Benutzerkennung ein Zugriff auf eine jeweilige Zugriffsklasse freigegeben wird.

7. Verfahren nach Anspruch 6,
dadurch gekennzeichnet,
daß als Freigabebedingung unter denen ein Zugriff auf eine jeweilige Zugriffsklasse erfolgt, ein einer anderen Benutzerkennung zugeordnetes Paßwort dient.

8. Verfahren nach einem der vorhergehenden Ansprüche,
dadurch gekennzeichnet,
daß mit der Administratorkennung eine Freigabe zum Rücksetzen von Paßwörtern der Benutzerkennungen erfolgt.

9. Verfahren nach einem der vorhergehenden Ansprüche,
dadurch gekennzeichnet,
daß als Freigabebedingung für mit der Administratorkennung jeweils ausführbaren Änderungen ein der Administrator-Überwacherkennung zugehöriges Paßwort dient.

10. Verfahren nach einem der vorhergehenden Ansprüche,
dadurch gekennzeichnet,
daß vom Steuerungssystem der Kommunikationsanlage eine zyklische Protokolldatei erstellt wird, in der wenigstens die während eines jeweiligen Zeitraumes mit der Administrator- und/oder AdministratorÜberwacher- und/oder Hersteller- und/oder Benutzerkennung vorgenommenen Änderungen vermerkt werden.

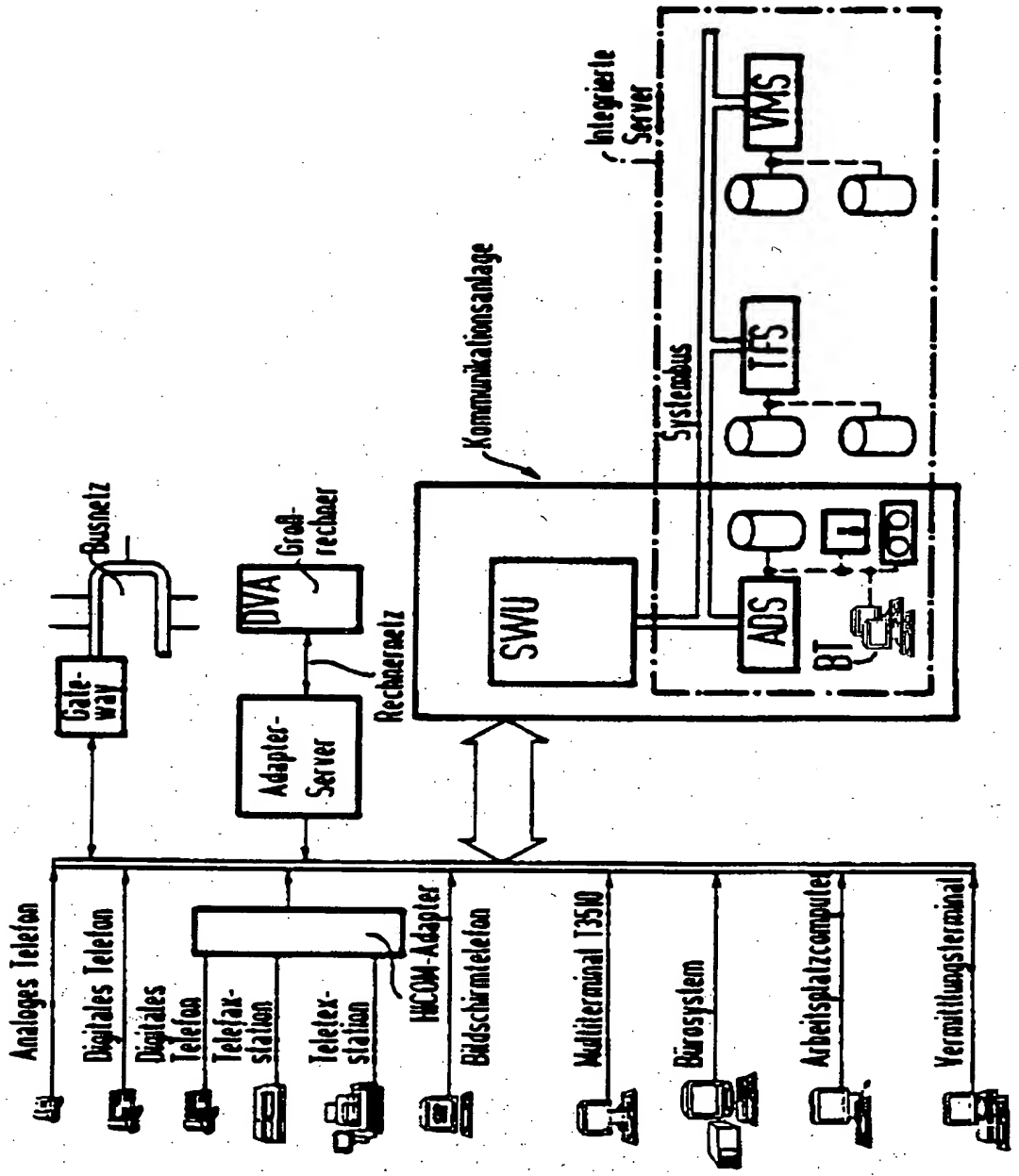

Analoges Telefon
Digitales Telefon
Digitales Telefon
Telefax-station
Teletex-station
HICOM-Adapter
Bildschirmtelefon
Multiterminal T3510
Bürosystem
Arbeitsplatzcomputer
Vermittlungsterminal
Gate-way
Busnetz
Adapter-Server
DVA
Groß-rechner
Rechnernetz
Kommunikationsanlage
SWU
Systembus
Integrierte Server
ADS
BT
TFS
VMS

FIG1

FIG 2

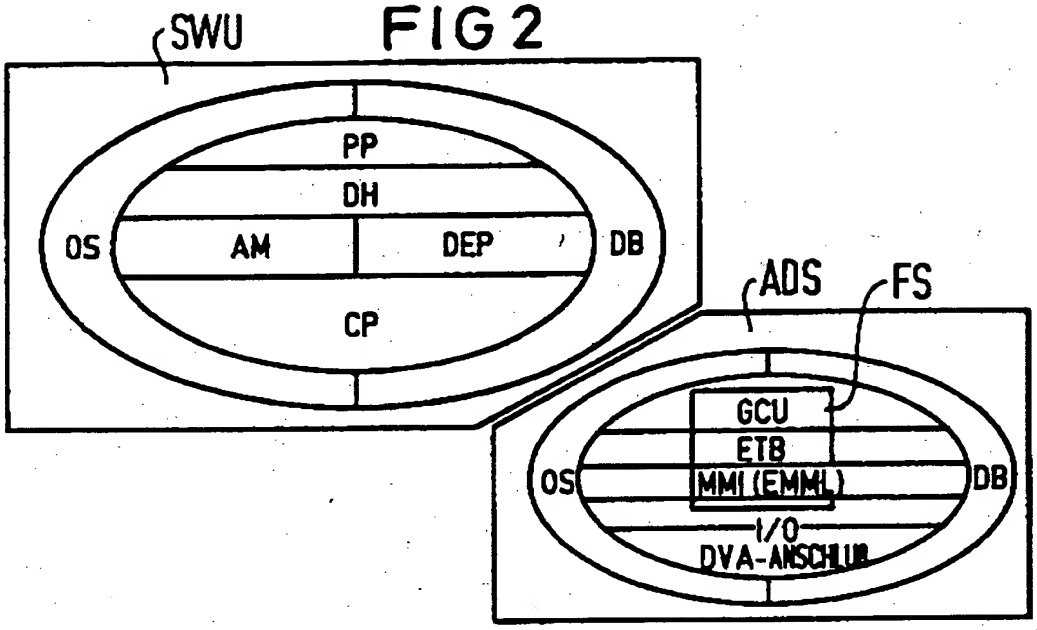


FIG 3

EMML Vx.xx	MAIN OBJEKTGRUPPEN	30.10. 13:15

LISTE DER OBJEKTGRUPPEN

ANLAGEN-HARDWARE
ANLAGEN-SOFTWARE
BEDIENGERÄTE
DATEN-KOMPLEX
GEBÜHRENERFASSUNG
TELESERVICE
LEISTUNGSMERKMALE
SATZ-KOMPLEX SWU
SYSTEMDATEN UND SWU-DATEN ALLG.
TEILNEHMER-KOMPLEX SWU
• TEXT- UND FAXSERVERDATEN TFS

BITTE EINE OBJEKTGRUPPE SELEKTIEREN

KENNUNG : " KUNDENDIENSTKENNUNG " SELECT

FIG4

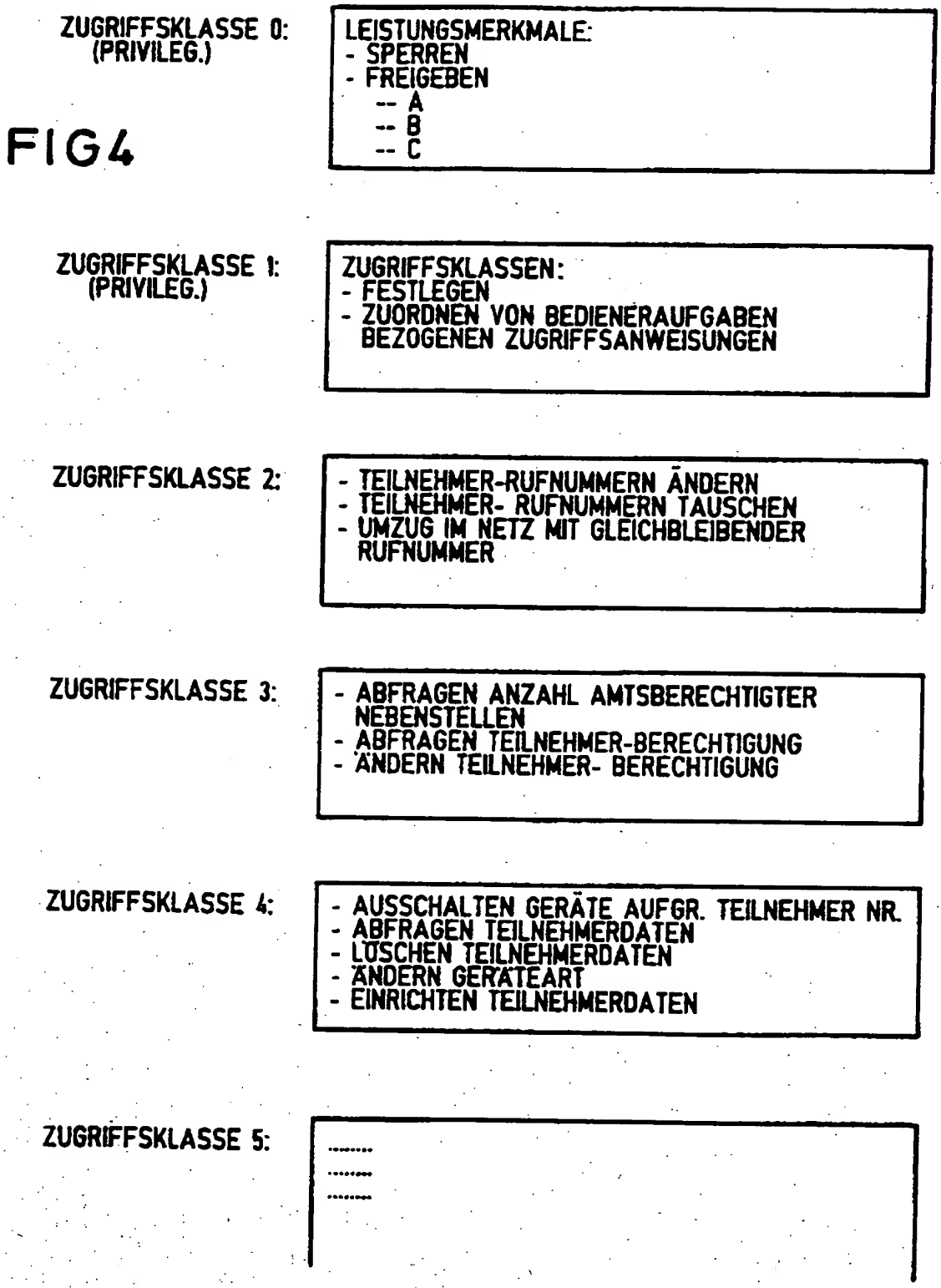

ZUGRIFFSKLASSE 0: (PRIVILEG.)
LEISTUNGSMERKMALE:
- SPERREN
- FREIGEBEN
-- A
-- B
-- C
ZUGRIFFSKLASSE 1: (PRIVILEG.)
ZUGRIFFSKLASSEN:
- FESTLEGEN
- ZUORDNEN VON BEDIENERAUFGABEN BEZOGENEN ZUGRIFFSANWEISUNGEN
ZUGRIFFSKLASSE 2:
- TEILNEHMER-RUFNUMMERN ÄNDERN
- TEILNEHMER- RUFNUMMERN TAUSCHEN
- UMZUG IM NETZ MIT GLEICHBLEIBENDER RUFNUMMER
ZUGRIFFSKLASSE 3:
- ABFRAGEN ANZAHL AMTSBERECHTIGTER NEBENSTELLEN
- ABFRAGEN TEILNEHMER-BERECHTIGUNG
- ÄNDERN TEILNEHMER- BERECHTIGUNG
ZUGRIFFSKLASSE 4:
- AUSSCHALTEN GERÄTE AUFGR. TEILNEHMER NR.
- ABFRAGEN TEILNEHMERDATEN
- LÖSCHEN TEILNEHMERDATEN
- ÄNDERN GERÄTEART
- EINRICHTEN TEILNEHMERDATEN
ZUGRIFFSKLASSE 5:
.....
.....
.....

FIG 5

HERSTELLERKENNUNG — PAßWORT

⟹ FREIGABE FÜR
- ZUGRIFFSKLASSE 0
- PAßWORTSPERRE RÜCKSETZEN FÜR ADMINISTRATOR UND ADMINISTRATOR ÜBERWACHUNG
- PAßWORTSTRATEGIE FESTLEGEN
- LOGFILE LESEN

ADMINISTRATORKENNUNG — PAßWORT

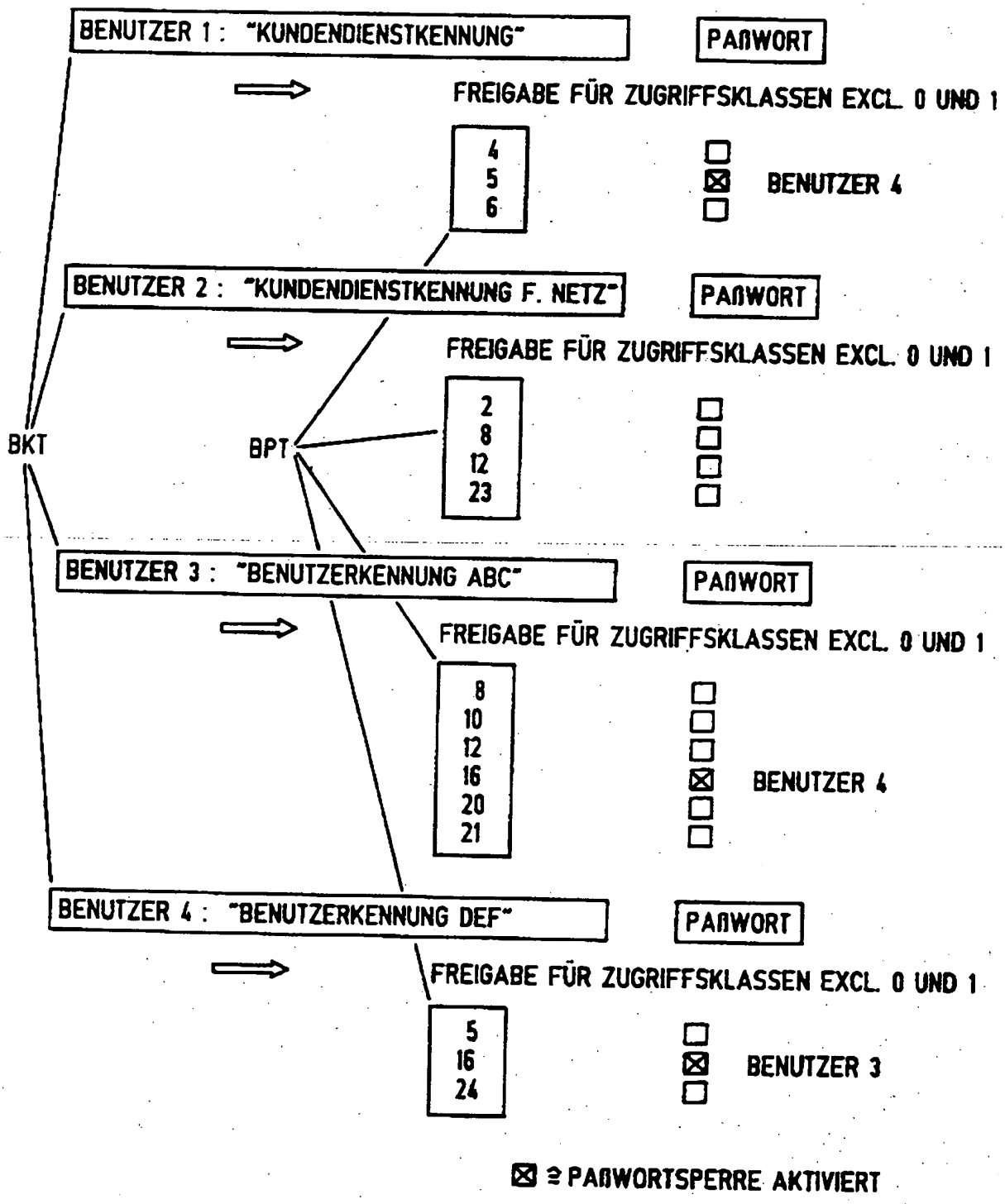
⟹ FREIGABE FÜR
- ☒ - BENUTZER (KENNUNG) 1, ..., n FESTLEGEN
- ☐ - ZUGRIFFSKLASSEN PRO BENUTZER FESTLEGEN
- ☐ - PAßWORTSPERRE RÜCKSETZEN FÜR BENUTZER 1, ..., n
- ☐ - ZUSÄTZLICHE PAßWORTSPERRE FÜR ZUGRIFFSKLASSE x DES BENUTZERS y FESTLEGEN
- ☐ - ZUGRIFFSKLASSEN 1, ..., m
- ☒ - LOGFILE LESEN UND SICHERN
- ☒ - KUNDENDATEIEN SICHERN

ADMINISTRATORÜBERWACHERKENNUNG — PAßWORT

⟹ FREIGABE FÜR
- PAßWORTSPERREN ZU KOMMANDOS UNTER ADMINISTRATORKENNUNG FESTLEGEN
- BENUTZER (KENNUNG) 1, ..., n LESEN
- LOGFILE LESEN UND SICHERN
- ZUGRIFFSKLASSEN 2, ..., m

☒ ≙ PAßWORTSPERRE AKTIVIERT

FIG 6


BENUTZER 1 : "KUNDENDIENSTKENNUNG"
PAßWORT
FREIGABE FÜR ZUGRIFFSKLASSEN EXCL. 0 UND 1
4
5
6
BENUTZER 4
BENUTZER 2 : "KUNDENDIENSTKENNUNG F. NETZ"
PAßWORT
FREIGABE FÜR ZUGRIFFSKLASSEN EXCL. 0 UND 1
BKT
BPT
2
8
12
23
BENUTZER 3 : "BENUTZERKENNUNG ABC"
PAßWORT
FREIGABE FÜR ZUGRIFFSKLASSEN EXCL. 0 UND 1
8
10
12
16
20
21
BENUTZER 4
BENUTZER 4 : "BENUTZERKENNUNG DEF"
PAßWORT
FREIGABE FÜR ZUGRIFFSKLASSEN EXCL. 0 UND 1
5
16
24
BENUTZER 3
☒ ≙ PAßWORTSPERRE AKTIVIERT

Europäisches Patentamt

EUROPÄISCHER RECHERCHENBERICHT

Nummer der Anmeldung

EP 92 10 3482

EINSCHLÄGIGE DOKUMENTE

Kategorie	Kennzeichnung des Dokuments mit Angabe, soweit erforderlich, der maßgeblichen Teile	Betrifft Anspruch	KLASSIFIKATION DER ANMELDUNG (Int. Cl.5)
A	US-A-4 959 856 (BISCHOFF ET AL.) * Spalte 6, Zeile 7 - Zeile 19; Abbildungen 2-5 *	1	H04Q11/04 H04Q3/545 H04M3/42
A	INT. CONF. ON COMMUNICATIONS '88, SESSION 35, PAPER 2 Bd. 2, 12. Juni 1988, PHILADELPHIA US Seiten 1 - 7 J.G.BRINSFIELD * Seite 4, linke Spalte, Zeile 33 - Zeile 57 *	1,10	
A	US-A-5 003 595 (COLLINS ET AL.) * das ganze Dokument *	1	
A	INT. SWITCHING SYMP. 1990, SESSION B10, PAPER #3 Bd. 6, 28. Mai 1990, STOCKHOLM SE Seiten 125 - 130 K. PRESTTUN ET AL.		

RECHERCHIERTE SACHGEBIETE (Int. Cl.5)
H04Q

Der vorliegende Recherchenbericht wurde für alle Patentansprüche erstellt

Recherchenort	Abschlußdatum der Recherche	Prüfer
DEN HAAG	17 SEPTEMBER 1992	KURVERS F.J.J.

KATEGORIE DER GENANNTEN DOKUMENTE

X : von besonderer Bedeutung allein betrachtet
Y : von besonderer Bedeutung in Verbindung mit einer anderen Veröffentlichung derselben Kategorie
A : technologischer Hintergrund
O : nichtschriftliche Offenbarung
P : Zwischenliteratur

T : der Erfindung zugrunde liegende Theorien oder Grundsätze
E : älteres Patentdokument, das jedoch erst am oder nach dem Anmeldedatum veröffentlicht worden ist
D : in der Anmeldung angeführtes Dokument
L : aus andern Gründen angeführtes Dokument

& : Mitglied der gleichen Patentfamilie, übereinstimmendes Dokument